

## CLAIMS

1. System for the secure and distributed management of a local  
5 community representation within network devices, characterized in that each network device (x) contains:

a provable identity ( $id_x$ ) or means to generate or to obtain a provable identity;

objects ( $MT(x)$ ,  $UT(x)$ ,  $DT(x)$ ) capable of memorizing identities of  
10 devices of the community having trust relationships with said device; and

means for establishing a protocol for trust relationships synchronization.

2. System according to claim 1, wherein each network device (x)  
15 contains:

one first object ( $MT(x)$ ) capable of memorizing identities of devices trusted by said device (x) and trusting said device (x);

one second object ( $UT(x)$ ) capable of memorizing identities of devices trusted by said device (x); and

20 one third object ( $DT(x)$ ) capable of memorizing identities of devices distrusted by said device (x).

3. System according to claim 2, wherein each network device (x) is furthermore designed to memorize proofs ( $S_j(id_x)$ ) received from other devices  
25 (j) of the community that said device (x) is trusted by other devices (j).

4. System according to claim 3 wherein said proofs ( $S_j(id_x)$ ) received from other devices of the community are stored in the first object ( $MT(x)$ ).

30 5. System according to one of claims 2 to 4 wherein each network device (x) is furthermore able to perform an operation to banish another device (y) of said community if the identity ( $id_y$ ) of said device to be banished is contained in the first ( $MT(x)$ ) or the second object ( $UT(x)$ ) of said network device (x), said banish operation consisting in removing the identity ( $id_y$ ) of said device  
35 to be banished from said first ( $MT(x)$ ) or second object ( $UT(x)$ ) and inserting said identity ( $id_y$ ) in said third object ( $DT(x)$ ) of said network device.